

# RFC-0005 Minimum Assessment Scope Standard

Thursday, April 24, 2025

*Note: The Minimum Assessment Scope was formerly referred to as the FedRAMP Boundary Policy / Boundary Guidance*

---

## Background

[OMB Circular A-130: Managing Information as a Strategic Resource](#) section 10 states that an “Authorization boundary” includes *“all components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.”* and further adds in footnote 64 that *“Agencies have significant flexibility in determining what constitutes an information system and its associated boundary.”*

[NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#) chapter 2.4 footnote 36 similarly states that *“the term authorization boundary is now used exclusively to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an authorizing official (i.e., the scope of the authorization).”*

[The FedRAMP Authorization Act \(44 USC § 3607 \(b\) \(7\)\)](#) defines “FedRAMP authorization” as *“a certification that a cloud computing product or service has ... completed a FedRAMP authorization process, as determined by the Administrator [of the General Services Administration]”* This responsibility is [delegated to the FedRAMP Director](#).

## Introduction

This standard moves FedRAMP away from reusing terminology and definitions designed for traditional information systems that often included a physical or logical “boundary” to contain information flow. FedRAMP is establishing a cloud-native approach to security assessment and authorization of cloud service offerings and their application and use within federal agency authorization boundaries.

FedRAMP authorization is certification that a cloud service has completed a FedRAMP assessment process to collect essential security information that shall be presumed adequate for use by federal agency authorizing officials making formal authorization decisions. FedRAMP authorization is not authorization to operate because agency authorizing officials are entirely responsible for reviewing and authorizing the operation of cloud services based on their own use case and environment.

FedRAMP asserts that tying FedRAMP authorizations to an “authorization boundary” creates confusion because the boundary specified in an agency’s authorization to operate a cloud service will always include additional resources related to the agency’s environment of operations. Agencies must follow OMB and NIST guidance to establish an appropriate authorization boundary for agency information systems that use FedRAMP authorized or certified cloud services.

This updated standard creates a standardized FedRAMP Minimum Assessment Scope that rescinds and replaces ALL previous guidance related to the boundaries of all FedRAMP authorizations and certifications, including the current Rev 5 Agency Authorization process and FedRAMP 20x. Best practices and technical assistance for following the FedRAMP Minimum Assessment Scope will be published separately.

## Definitions

The following definitions apply to all FedRAMP materials:

- a. **"Federal information"** has the meaning as defined in [OMB Circular A-130](#) and any successor documents. As of Apr 2025, this means *"information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the federal government, in any medium or form."*
- b. **"Information resources"** is defined in [44 USC § 3502 \(6\)](#) as *"information and related resources, such as personnel, equipment, funds, and information technology."* This applies to any aspect of the cloud service offering, both technical and managerial, including everything that makes up the business of the offering from organizational policies and procedures to hardware, software, and code.

## FedRAMP Minimum Assessment Scope

The FedRAMP Minimum Assessment Scope establishes the fundamental requirements for all aspects of a cloud service provider and cloud service offering that **MUST** be included within the boundary of a FedRAMP assessment and authorization package.

The Minimum Assessment Scope includes all information resources managed by a cloud service provider and their cloud service offering that:

1. Handle federal information; and/or
2. Likely impact confidentiality, integrity, or availability of federal information

## Application of Minimum Assessment Scope

The following statements provide additional clarification on applying the Minimum Assessment Scope for FedRAMP:

- A. Information resources and metadata that do not meet condition (1) or (2) are outside the Minimum Assessment Scope.

- B. If the cloud service uses information resources from other FedRAMP authorized or certified services then only the configuration and usage of those information resources is included in the Minimum Assessment Scope.
- C. If the cloud service uses information resources from other services that are not FedRAMP authorized or certified then all aspects of those services where (1) or (2) applies are included in the Minimum Assessment Scope.
- D. Software and other such products (including agents and clients) that are installed, managed, and operated on agency information systems are outside the scope of FedRAMP. Any information resources in the cloud service that control or communicate with such products are within the Minimum Assessment Scope if (1) or (2) applies.
- E. Information resources of the service offering may vary by impact level as appropriate to the level of information handled or impacted by the information resource so long as this is clearly identified and documented.
- F. Stakeholders should review best practices and technical assistance provided separately by FedRAMP for help with applying the Minimum Assessment Scope as needed.